



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/818,074	03/26/2001	W. Dale Hopkins	20206-15 (P00-3323)	9764

7590 03/16/2005

Hewlett-Packard Company
Attn. Bill Streeter
Intellectual Property Administration
P.O. Box 272400
Fort Collins, CO 80527-2400

EXAMINER

NALVEN, ANDREW L

ART UNIT	PAPER NUMBER
----------	--------------

2134

DATE MAILED: 03/16/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/818,074

Applicant(s)

HOPKINS ET AL.

Examiner

Andrew L. Nalven

Art Unit

2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 26 March 2001.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-3,5-18,20 and 22-53 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☒ Claim(s) 1-3,5-18,20 and 22-48 is/are allowed.
- 6) ☒ Claim(s) 49 and 50 is/are rejected.
- 7) ☒ Claim(s) 51-53 is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 26 March 2001 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. Claims 1-3, 5-18, 20, 22-53 are pending.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

2. Claims 49-50 are rejected under 35 U.S.C. 103(a) as being unpatentable over Boesch US Patent No. 6,125,185 in view of Hori et al US Patent No. 6,578,057.
3. With regards to claim 49, Boesch teaches a processor, a memory coupled to the processor, the memory used to store a set of cryptographic parameters (Boesch, column 5 lines 1-5), wherein the processor receives a request from a second computer for a cryptographic parameter, said request includes a specified cryptographic parameter characteristic (Boesch, column 5 lines 13-20), and wherein the processor provides the requested cryptographic parameter in response to the request (Boesch, column 5 lines 13-15, column 4 lines 51-67). Boesch fails to teach the storing of parameters usable to generate a cryptographic key. Hori teaches the storing of parameters usable to generate a cryptographic key (Hori, column 4 lines 46-65). At the time the invention was made, it would have been obvious to a person of ordinary skill in

Art Unit: 2134

the art to utilize Hori's method of prime number generation with Boesch's key generation system because it offers the advantage of providing a method of generating prime numbers that are beneficial for message authentication and user validation (Hori, column 1 lines 16-23).

4. With regards to claim 50, Boesch as modified teaches the cryptographic parameter being one or more distinct prime numbers (Hori, column 4 lines 46-65).

Allowable Subject Matter

5. Claims 1-3, 5-18, 20 and 22-48 are allowed.

6. Claims 51-53 objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

7. The following is a statement of reasons for the indication of allowable subject matter: See office action mailed 9 September 2004 for reasons for indicating allowable subject matter relating to claims 1-43.

8. With regards to claims 44-48, the cited prior art fails to teach or suggest the storing on a server of a set of cryptographic parameters suitable for generating a cryptographic key and providing the parameters to allow generating at the client the a

Art Unit: 2134

cryptographic key using the provided cryptographic parameter. As such, the cited prior art fails to anticipate or render obvious the above-cited claims.

9. With regards to claim 51, the cited prior art fails to teach or suggest the specified cryptographic characteristic being a number indicative of how many of the one or more distinct randomly generated prime numbers are requested. As such, the cited prior art fails to anticipate or render obvious the above-cited claim.

10. With regards to claim 52, the cited prior art fails to teach or suggest the specified cryptographic characteristic being a modulus generated from a plurality of distinct randomly generated prime numbers. As such, the cited prior art fails to anticipate or render obvious the above-cited claim.

Conclusion

11. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any

Art Unit: 2134

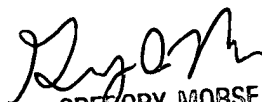
extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

12. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Andrew L Nalven whose telephone number is 571 272 3839. After October 26, 2004, Examiner can be reached at 571 272 – 3839. The examiner can normally be reached on Monday - Thursday 8-6, Alternate Fridays.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached on 571 272 3838. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Andrew Nalven



GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100